

The invention claimed is:

1 1. A method comprising:

2 receiving a request from a client at a network address translator (NAT)
3 that defines for a protocol not directly supported by the NAT a generalized port
4 number (GPN) associated with that unsupported protocol and its location in each
5 packet;

6 creating an entry in a translation table of the NAT that defines for that
7 protocol an association between a client's private IP address and GPN, a NAT's
8 assigned global IP address and GPN, and a foreign IP address, said entry being
9 used for translating in outgoing packets received by the NAT from the client
10 using that protocol and having the foreign IP address as their destination, the
11 client's private source IP address and GPN to the NAT's global IP address and
12 GPN, respectively, and for translating in incoming packets sent from the foreign
13 IP address using that protocol to the NAT's global destination IP address and
14 GPN, the NAT's global destination IP address and GPN to the client's private
15 destination IP address and GPN, respectively.

1 2. A method comprising:

2 receiving a request from a client at a network address translator (NAT)
3 that defines for a protocol not directly supported by the NAT a generalized port
4 number (GPN) associated with that unsupported protocol and its location in each
5 packet;

6 creating an entry in a translation table of the NAT that defines for that
7 protocol an association between a client's private IP address and GPN, NAT's
8 assigned global IP address and GPN, and a foreign IP address; and

9 in outgoing packets received by the NAT from the client using that
10 protocol and having the foreign IP address as their destination, translating in

3. A method comprising:

receiving a request from a client at a network address translator (NAT) that defines for a protocol not directly supported by the NAT a generalized port number (GPN) associated with that unsupported protocol and its location in each packet;

9 in incoming packets received by the NAT and sent from the foreign IP
10 address using that protocol to the NAT's global destination IP address and GPN,
11 translating in accordance with the entry, the NAT's global destination IP address
12 and GPN to the client's private destination IP address and GPN, respectively.

1 5. The method of claims 1, 2 or 3 wherein the unsupported protocol is a
2 protocol in the IP Security (IPSec) security protocol suite.

1 7. The method of claim 6 wherein the leased initiator cookie is chosen by
2 the NAT to be used as both the client's GPN and the NAT's GPN.

26

1 11. A network address translator (NAT) comprising:
2 means for receiving a request from a client at a network address
3 translator (NAT) that defines for a protocol not directly supported by the NAT a
4 generalized port number (GPN) associated with that unsupported protocol and
5 its location in each received packet;
6 memory means for storing a translation table;

7
8
9

10
11
12
13

1

2
3
4

5

6
7
8

9
10
11
12
13

1
2

- 1
- 2

1
2

3 (ISAKMP) and the GPN is an initiator cookie leased from the NAT to be unique
4 to the client.

1 16. The NAT of claim 15 wherein the leased initiator cookie is chosen by
2 the NAT to be used as both the client's GPN and the NAT's GPN.

1 17. The NAT of claim 14 wherein the unsupported protocol in the IPsec
2 security suite is the AH or ESP protocols in tunnel or transport modes, and the
3 GPN is an incoming Security Parameter Index (SPI) leased from the NAT to be
4 unique to the client.

1 18. The NAT of claim 17 wherein the leased SPI is chosen by the NAT to
2 be used as both the client's GPN and the NAT's GPN.

1 19. A computer readable media tangibly embodying a program of
2 instructions executable by a computer to perform a method at a network address
3 translator (NAT), the method comprising:

4 receiving a request from a client that defines for a protocol not directly
5 supported by the NAT a generalized port number (GPN) associated with that
6 unsupported protocol and its location in each packet;

7 creating an entry in a translation table of the NAT that defines for that
8 protocol an association between a client's private IP address and GPN, a NAT's
9 assigned global IP address and GPN, and a foreign IP address, said entry being
10 used for translating in outgoing packets received by the NAT from the client
11 using that protocol and having the foreign IP address as their destination, the
12 client's private source IP address and GPN to the NAT's global IP address and
13 GPN, respectively, and for translating in incoming packets sent from the foreign
14 IP address using that protocol to the NAT's global destination IP address and
15 GPN, the NAT's global destination IP address and GPN to the client's private
16 destination IP address and GPN, respectively.

1 20. A computer readable media tangibly embodying a program of
2 instructions executable by a computer to perform a method at a network address
3 translator (NAT), the method comprising:

4 receiving a request from a client that defines for a protocol not directly
5 supported by the NAT a generalized port number (GPN) associated with that
6 unsupported protocol and its location in each packet;

7 creating an entry in a translation table of the NAT that defines for that
8 protocol an association between a client's private IP address and GPN, NAT's
9 assigned global IP address and GPN, and a foreign IP address; and

in outgoing packets received by the NAT from the client using that protocol and having the foreign IP address as their destination, translating in accordance with the entry, the client's private source IP address and GPN to the NAT's global IP address and GPN, respectively.

21. A computer readable media tangibly embodying a program of instructions executable by a computer to perform a method at a network address translator (NAT), the method comprising:

4 receiving a request from a client that defines for a protocol not directly
5 supported by the NAT a generalized port number (GPN) associated with that
6 unsupported protocol and its location in each packet;

7 creating an entry in a translation table of the NAT that defines for that
8 protocol an association between a client's private IP address and GPN, a NAT's
9 assigned global IP address and GPN, and a foreign IP address; and

in incoming packets received by the NAT and sent from the foreign IP address using that protocol to the NAT's global destination IP address and GPN, translating in accordance with the entry, the NAT's global destination IP address and GPN to the client's private destination IP address and GPN, respectively.

1 27. The method of claim 26 wherein the leased SPI is chosen by the NAT
2 to be used as both the client's GPN and the NAT's GPN.